Highly asymmetric quantum cloning in arbitrary dimension

Jaromír Fiurášek,[1,2] Radim Filip,[1] and Nicolas J. Cerf[2]

[1]*Department of Optics, Palacký University, 17. listopadu 50, 77200 Olomouc, Czech Republic*
[2]*QUIC, Ecole Polytechnique, CP 165, Université Libre de Bruxelles, 1050 Bruxelles, Belgium*

We investigate the universal asymmetric cloning of states in a Hilbert space of arbitrary dimension. We derive the class of optimal and fully asymmetric $1 \to 3$ cloners, which produce three copies, each having a different fidelity. A simple parametric expression for the maximum achievable cloning fidelity triplets is then provided. As a side-product, we also prove the optimality of the $1 \to 2$ asymmetric cloning machines that have been proposed in the literature.

PACS numbers: 03.67.-a, 03.65.-w

I. INTRODUCTION

Quantum information theory exploits the laws of quantum mechanics to devise novel means of processing, manipulating and transmitting information. Among the most celebrated applications one finds quantum computing and quantum cryptography. The latter allows a secure key distribution among two distant partners, the security of the distributed key being guaranteed by the laws of quantum mechanics [1]. In particular, the linearity of quantum mechanics implies that an unknown quantum state cannot be copied [2]. Thus any attempt by an eavesdropper to learn about the state transmitted from the sender to the receiver will unavoidably introduce some noise, which can be detected at the receiver's station.

Although perfect copying is forbidden it is still possible to carry out an approximate cloning of quantum states. This issue has attracted a lot of attention during the recent years and the optimal universal symmetric cloning machines which produce M approximate copies out of N inputs have been found [3, 4, 5, 6, 7, 8]. In the context of quantum cryptography, one is particularly interested in the asymmetric cloning machines which produce two clones with different fidelities [9, 10, 11, 12, 13, 14]. This allows one to study the interplay between the information gained by an eavesdropper and the noise introduced in the channel. Importantly, the asymmetric cloning proved to be a very efficient (or even optimal) individual eavesdropping attack on certain kinds of QKD protocols [15, 16, 17, 18]. Recently, optimal asymmetric $1 \to 2$ cloning of qubits encoded as polarization states of single photons has been demonstrated experimentally [19].

However, the universal asymmetric cloning machines considered in the literature [9, 10, 11, 12] are only conjectured to be optimal, and so far the proof of optimality has been missing (except for the qubit case [10]). In this paper, we provide such a proof. We will then go beyond the $1 \to 2$ asymmetric cloning and shall consider a novel class of universal asymmetric machines which produce three clones, each of them with possibly different fidelity. These machines were recently proposed and briefly discussed in Ref. [20] which introduced the general concept of a fully asymmetric $N \to M$ cloning machine producing M approximate clones with M different fidelities. In this paper we expand this discussion and derive explicitly the optimal cloning transformation, present the details of the optimality proof, and provide a simple parametric description of the optimal universal asymmetric $1 \to 3$ cloning machines in arbitrary dimensions. We expect that our findings will play an important role in investigations of multi-party quantum communication protocols and quantum information distribution in quantum networks. An independent similar study of multipartite asymmetric cloning of qubits is reported in [21].

The paper is structured as follows. In Section II we prove the optimality of the universal $1 \to 2$ asymmetric cloning machines for qudits. In Section III we investigate the fully asymmetric optimal universal quantum triplicators which produce three approximate clones with three different fidelities. Finally, Section IV contains a brief summary and conclusions.

II. ASYMMETRIC QUANTUM DUPLICATORS

Let us begin by briefly reviewing an isomorphism between completely positive maps $\mathcal{S}$ and positive semidefinite operators $S \geq 0$ on the tensor product of the input and output Hilbert spaces of map $\mathcal{S}$, denoted respectively as $\mathcal{H}_{in}$ and $\mathcal{H}_{out}$. Consider a maximally entangled state on $\mathcal{H}_{in}^{\otimes 2}$,

$$|\Phi^+\rangle = \frac{1}{\sqrt{d}} \sum_{j=1}^{d} |j\rangle|j\rangle \tag{1}$$

with $d = \dim(\mathcal{H}_{in})$. If the map $\mathcal{S}$ is applied to the second subsystem while nothing happens to the first one, the resulting (generally mixed) quantum state contains all the information about the map. Qualitatively speaking, if we project the first subsystem onto the (complex conjugate of the) input state so that the second subsystem is projected onto the input state, then, after applying $\mathcal{S}$, it is left in the corresponding output state. The first subsystem is therefore conventionally called the reference system, denoted with the subscript R, since it keeps a memory of the state that was processed in the channel.

Mathematically, the positive semidefinite operator

$$S = \mathcal{I} \otimes \mathcal{S}(d\,\Phi^+_{RO}) \tag{2}$$

is therefore isomorphic to the map $\mathcal{S}$, where the subscript O denotes here the output system, $\Phi^+ = |\Phi^+\rangle\langle\Phi^+|$, and the prefactor d has been introduced for normalization purposes. The fact that the map $\mathcal{S}$ is trace preserving indeed implies the condition

$$\mathrm{Tr}_O[S] = \mathbb{1}_R. \tag{3}$$

The map $\mathcal{S}$ can be expressed in terms of S as

$$\rho \to \mathcal{S}(\rho) = \mathrm{Tr}_R[\rho_R^T \otimes \mathbb{1}_O\, S], \tag{4}$$

where T denotes the transposition in the Schmidt basis of state $|\Phi^+\rangle$.

Let us now assume that S describes the $1 \to 2$ cloning transformation of qudits. The output Hilbert space is endowed with tensor product structure, $\mathcal{H}_{out} = \mathcal{H}_A \otimes \mathcal{H}_B$, where the subscripts A and B label the two clones. For each particular input state $|\psi\rangle$, we can calculate the fidelity of each clone as follows,

$$\begin{aligned} F_A(\psi) &= \mathrm{Tr}(\psi_R^T \otimes \psi_A \otimes \mathbb{1}_B\, S), \\ F_B(\psi) &= \mathrm{Tr}(\psi_R^T \otimes \mathbb{1}_A \otimes \psi_B\, S), \end{aligned} \tag{5}$$

where R labels the input system and $\psi \equiv |\psi\rangle\langle\psi|$ is a short hand notation for the density matrix of a pure state. We are usually interested in the average performance of the cloning machine, which can be quantified by the mean fidelities,

$$F_A = \int_\psi F_A(\psi)\, d\psi, \qquad F_B = \int_\psi F_B(\psi)\, d\psi, \tag{6}$$

where the measure $d\psi$ determines the kind of the cloning machines we are dealing with. Universal cloning machines which clone equally well all states from the input Hilbert space correspond to choosing $d\psi$ to be the Haar measure on the group $SU(d)$. The fidelities (6) are linear functions of the operator S,

$$F_A = \mathrm{Tr}[SL_A], \qquad F_B = \mathrm{Tr}[SL_B], \tag{7}$$

where the positive semidefinite operators L_j are given by

$$L_A = \int_\psi \psi_R^T \otimes \psi_A \otimes \mathbb{1}_B\, d\psi, \quad L_B = \int_\psi \psi_R^T \otimes \mathbb{1}_A \otimes \psi_B\, d\psi. \tag{8}$$

In case of universal cloning, the integral over $d\psi$ can be easily calculated with the help of Schur's lemma, and we get, for instance,

$$\begin{aligned} \int_\psi \psi_R^T \otimes \psi_A\, d\psi &= \frac{2}{d(d+1)} (\Pi^+_{RA})^{T_R} \\ &= \frac{1}{d(d+1)} [\mathbb{1}_R \otimes \mathbb{1}_A + d\,\Phi^+_{RA}]. \end{aligned}$$

Here, Π^+ denotes a projector onto symmetric subspace of two qudits, $d(d+1)/2$ is the dimension of this subspace, and T_R stands for transposition with respect to the subsystem R. Thus, we have

$$L_{A,B} = \frac{1}{d(d+1)} [\mathbb{1}_{RAB} + d\,\tilde{L}_{A,B}], \tag{9}$$

with

$$\tilde{L}_A = \Phi^+_{RA} \otimes \mathbb{1}_B, \qquad \tilde{L}_B = \Phi^+_{RB} \otimes \mathbb{1}_A. \tag{10}$$

The optimal asymmetric cloning machine S should maximize a convex mixture of the mean fidelities F_A and F_B [22, 23],

$$F = pF_A + (1-p)F_B = \mathrm{Tr}[SL], \tag{11}$$

where $L = pL_A + (1-p)L_B$ and p is a parameter that controls the asymmetry of the cloner. The maximization of F for a given value of p can be equivalently rephrased as a maximization of F_B for a fixed value of F_A. Suppose that we find S that maximizes F. It is then clear that for a given F_A this map yields maximum possible F_B, because any higher F_B would increase F. This explains why optimal asymmetric cloners can be found simply by maximizing the convex mixture of single-clone fidelities with variable mixing ratio.

The maximum achievable F is upper bounded by the maximum eigenvalue λ_{max} of the operator L [24]. Taking into account the trace-preservation condition, we have

$$F \le d\,\lambda_{max}. \tag{12}$$

Although this bound need not be saturated in general [24, 25], it is reached by the optimal asymmetric $1 \to 2$ universal cloning machines, as we shall show below. It follows that we have to calculate the eigenvalues of the operator

$$L = \frac{1}{d(d+1)} [\mathbb{1}_{RAB} + d\,\tilde{L}] \tag{13}$$

with

$$\tilde{L} = p\,\tilde{L}_A + (1-p)\,\tilde{L}_B. \tag{14}$$

We can neglect the trivial part of L which is proportional to the identity operator, and only need to investigate the eigenstates and eigenvalues of $\tilde{L}$. Luckily, this problem is greatly simplified by noting that $\tilde{L}$ has a support of dimension $2d$, spanned by $|\Phi^+\rangle_{RA}|k\rangle_B$ and $|\Phi^+\rangle_{RB}|k\rangle_A$. This implies that $\tilde{L}$ has at most $2d$ non-zero eigenvalues. Moreover, it turns out that there are only two d-fold degenerate eigenvalues, λ_1 and λ_2. The eigenstates have the following form,

$$|\lambda_j; k\rangle = \alpha\,|\Phi^+\rangle_{RA}|k\rangle_B + \beta\,|\Phi^+\rangle_{RB}|k\rangle_A, \tag{15}$$

where $j = 1, 2$ and $k = 1, \cdots, d$. The two eigenvalues $\lambda_1 > \lambda_2$ are roots of the quadratic equation

$$\lambda^2 - \lambda + p(1-p)[1 - d^{-2}] = 0 \tag{16}$$

and the ratio β/α, which fixes the eigenstate (15), can be expressed in terms of λ, p, and d as

$$\frac{\beta}{\alpha} = d(\lambda/p - 1). \tag{17}$$

Since λ is real, we can assume without loss of generality that α and β are both real and $\alpha \geq 0$. By properly normalizing the eigenstates $|\lambda_j; k\rangle$, we get

$$\alpha^2 + \beta^2 + \frac{2\alpha\beta}{d} = 1. \tag{18}$$

The optimal cloning transformation S is then simply the projector onto the d-dimensional sub-space spanned by the eigenstates $|\lambda_1; k\rangle$ corresponding to the maximum eigenvalue λ_1,

$$S = \sum_{k=1}^{d} |\lambda_1; k\rangle\langle\lambda_1; k|. \tag{19}$$

Note that $\lambda_1 > p$ hence both α and β in Eq. (15) are positive. One can easily check that $\mathrm{Tr}_{AB}[S] = \mathbb{1}_R$, hence S is a trace-preserving map.

Moreover, $F = d\,\lambda_{max}$ by construction, which proves the optimality. The fidelities of the optimal clones A and B can be obtained in terms of the coefficients α and β by noting first that

$$\begin{aligned} \langle\lambda_1; k|\tilde{L}_A\,|\lambda_1; k\rangle &= (\alpha + \beta/d)^2, \\ \langle\lambda_1; k|\tilde{L}_B\,|\lambda_1; k\rangle &= (\beta + \alpha/d)^2, \end{aligned} \tag{20}$$

so that, using Eq. (18), we get

$$\mathrm{Tr}[S\tilde{L}_A] = d - \frac{d^2-1}{d}\,\beta^2, \quad \mathrm{Tr}[S\tilde{L}_B] = d - \frac{d^2-1}{d}\,\alpha^2. \tag{21}$$

Therefore, we obtain for the fidelities of the asymmetric cloner

$$F_A = 1 - \frac{d-1}{d}\beta^2, \qquad F_B = 1 - \frac{d-1}{d}\alpha^2, \tag{22}$$

where α^2 and β^2 are the so-called depolarizing fractions as discussed in Ref. [9]. The expressions (18) and (22) exactly coincide with the formula characterizing the class of asymmetric cloning machines derived in [9], which therefore is optimal.

The optimal cloning map (19) can be realized unitarily by purifying S into the state

$$|\Phi\rangle = \alpha\,|\Phi^+\rangle_{RA}|\Phi^+\rangle_{BE} + \beta\,|\Phi^+\rangle_{RB}|\Phi^+\rangle_{AE}, \tag{23}$$

where E stands for an ancillary system, that is, we get S when tracing over E. The resulting isometry that transforms the input single-qudit state $|\psi\rangle$ onto the output state of three qudits (two clones and one anti-clone) can be written, by projecting the reference system R onto $|\psi^*\rangle$, as

$$|\psi\rangle \to \alpha\,|\psi\rangle_A|\Phi^+\rangle_{BE} + \beta\,|\psi\rangle_B|\Phi^+\rangle_{AE}. \tag{24}$$

III. ASYMMETRIC QUANTUM TRIPLICATORS

Having proved the optimality of the universal asymmetric $1 \to 2$ cloning machines, we now use the same techniques to construct the optimal universal asymmetric $1 \to 3$ cloners. These machines produce three clones, A, B, and C, each clone possibly having a different fidelity (F_A, F_B, and F_C). The optimal asymmetric cloning machine should maximize the cloning fidelities such that for a given pair of fidelities (say F_A and F_B) the fidelity of the third clone (F_C) is maximum.

The output Hilbert space of the asymmetric quantum triplicator is a tensor product of Hilbert spaces of the three clones. The average fidelity of jth clone can be again expressed as $F_j = \mathrm{Tr}[SL_j]$ with $j \in \{A, B, C\}$, where now

$$L_A = \frac{1}{d(d+1)}[\mathbb{1}_R \otimes \mathbb{1}_A + d\Phi^+_{RA}] \otimes \mathbb{1}_{BC}, \tag{25}$$

where R indicates the reference, and L_B and L_C can be obtained by cyclic permutation of A, B, C. In analogy with Eq. (11), the optimal asymmetric $1 \to 3$ cloning machine should maximize a convex combination of the three single-clone fidelities,

$$F = aF_A + bF_B + cF_C, \tag{26}$$

where $a + b + c = 1$, $a, b, c \geq 0$ and the asymmetry of the cloner is determined by the ratios a/b and a/c. The fidelity (26) can be rewritten as $F = \mathrm{Tr}[SL]$, where $L = aL_A + bL_B + cL_C$. Similarly as in the case of $1 \to 2$ cloning, we have to determine the eigenspace corresponding to the maximum eigenvalue of

$$L \;=\; \frac{1}{d(d+1)}\left[\mathbb{1}_{RABC} + d\,\tilde{L}\right], \tag{27}$$

where

$$\tilde{L} = a\,\Phi^+_{RA} \otimes \mathbb{1}_{BC} + b\,\Phi^+_{RB} \otimes \mathbb{1}_{AC} + c\,\Phi^+_{RC} \otimes \mathbb{1}_{AB}. \tag{28}$$

Due to the high symmetry, the operator $\tilde{L}$ has only six different non-zero eigenvalues. Three of them are $d(d+1)/2$-fold degenerate and the corresponding eigenstates read,

$$\begin{aligned} |\lambda_+; kl\rangle \;=\; & \alpha\,|\Phi^+\rangle_{RA}|kl^+\rangle_{BC} + \beta\,|\Phi^+\rangle_{RB}|kl^+\rangle_{AC} \\ & +\gamma\,|\Phi^+\rangle_{RC}|kl^+\rangle_{AB}, \end{aligned} \tag{29}$$

with $l \geq k$. Here we take $|kl^+\rangle = (|kl\rangle + |lk\rangle)/\sqrt{2}$ if $k \neq l$, while $|kk^+\rangle = |kk\rangle$. The three eigenvalues ($\lambda_{+,1} > \lambda_{+,2} > \lambda_{+,3}$) can be determined as roots of the cubic equation

$$\begin{aligned} P_+(\lambda_+) \;\equiv\; & \lambda_+^3 - \lambda_+^2 + \lambda_+(ab + bc + ac)\left(1 - d^{-2}\right) \\ & -abc\left(1 + 2d^{-3} - 3d^{-2}\right) = 0, \end{aligned} \tag{30}$$

and the coefficients α, β, γ can be expressed in terms of a, b, c, and λ_+ by solving the system of linear equations

$$\begin{aligned}(\lambda_+ - a)\alpha - \frac{a}{d}(\beta+\gamma) = 0,\\ (\lambda_+ - b)\beta - \frac{b}{d}(\alpha+\gamma) = 0,\\ (\lambda_+ - c)\gamma - \frac{c}{d}(\alpha+\beta) = 0.\end{aligned} \tag{31}$$

The normalization of the eigenstate $|\lambda_+; kl\rangle$ imposes the constraint

$$\alpha^2 + \beta^2 + \gamma^2 + \frac{2}{d}(\alpha\beta + \alpha\gamma + \beta\gamma) = 1. \tag{32}$$

The other three eigenvalues correspond to the anti-symmetric combinations of $|kl\rangle$ and $|lk\rangle$, that is, $|kl^-\rangle = (|kl\rangle - |lk\rangle)/\sqrt{2}$, and are thus $d(d-1)/2$-fold degenerate. The eigenstates are given by

$$\begin{aligned}|\lambda_-; kl\rangle \;=\; &\alpha|\Phi^+\rangle_{RA}|kl^-\rangle_{BC} + \beta|\Phi^+\rangle_{RB}|kl^-\rangle_{AC}\\ &+\gamma|\Phi^+\rangle_{RC}|kl^-\rangle_{AB},\end{aligned} \tag{33}$$

with $l > k$, and the cubic equation for the eigenvalues λ_- reads

$$\begin{aligned}P_-(\lambda_-) \;\equiv\; &\lambda_-^3 - \lambda_-^2 + \lambda_-(ab+bc+ac)\left(1-d^{-2}\right)\\ &-abc\left(1-2d^{-3}-3d^{-2}\right) = 0.\end{aligned} \tag{34}$$

Since the polynomials $P_+(\lambda)$ and $P_-(\lambda)$ differ only in their zeroth order terms, their graphs look identical up to a vertical shift of $4abc/d^3$. This simple geometrical observation reveals that the maximum eigenvalue $\lambda_{+,1}$ is always larger than the maximum eigenvalue $\lambda_{-,1}$. Hence, in determining the optimal cloning transformation, which corresponds to the maximum eigenvalue of (27), we have to consider only the eigenstates (29). It follows from the structure of the operator $\tilde{L}$ that $\lambda_{+,1} \geq \max(a, b, c)$. This, together with Eq. (31) implies that the coefficients α, β, and γ of an eigenstate corresponding to the maximum eigenvalue $\lambda_{+,1}$ must be all positive (or all negative). The optimal trace-preserving $1 \to 3$ cloning map can then be expressed simply as the properly normalized projector onto the subspace spanned by the $d(d+1)/2$ eigenstates (29) with eigenvalue $\lambda_{+,1}$,

$$S = \frac{2}{d+1}\sum_{l\geq k} |\lambda_{+,1}; kl\rangle\langle\lambda_{+,1}; kl|, \tag{35}$$

where the prefactor originates from the constraint that $\mathrm{Tr}(S) = d$. A unitary implementation of this CP map requires two ancilla systems, E and F, and can be characterized by the purification of S, namely

$$\begin{aligned}|\Phi\rangle \;=\; &\sqrt{d}\,\mathcal{C}\left[\alpha\,|\Phi^+\rangle_{RA}(|\Phi^+\rangle_{BE}|\Phi^+\rangle_{CF} + |\Phi^+\rangle_{BF}|\Phi^+\rangle_{CE})\right.\\ &+\beta\,|\Phi^+\rangle_{RB}(|\Phi^+\rangle_{AE}|\Phi^+\rangle_{CF} + |\Phi^+\rangle_{AF}|\Phi^+\rangle_{CE})\\ &\left.+\gamma\,|\Phi^+\rangle_{RC}(|\Phi^+\rangle_{AE}|\Phi^+\rangle_{BF} + |\Phi^+\rangle_{AF}|\Phi^+\rangle_{BE})\right],\end{aligned}$$

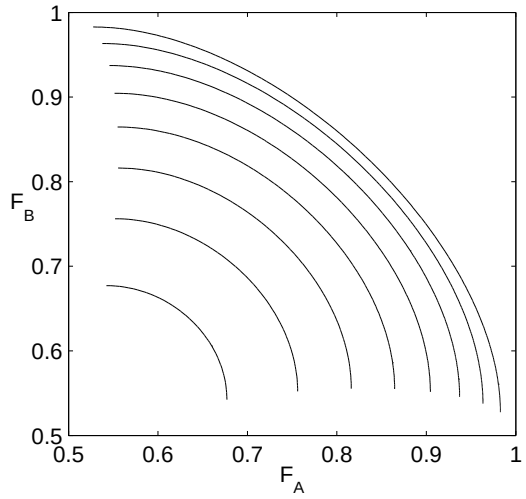

FIG. 1: The trade-off between the fidelities F_A and F_B for a fixed fidelity F_C is shown for the optimal universal asymmetric $1 \to 3$ cloning of qubits. The curves are plotted for several different values of $F_C(n) = 0.6 + 0.05n$, $n = 0, \ldots, 7$, the most inward curve corresponding to the highest value of F_C.

where we have used the identity

$$\begin{aligned}\frac{2}{d}\sum_{l\geq k}|kl^+\rangle_{BC}|kl^+\rangle_{EF} =\\ |\Phi^+\rangle_{BE}|\Phi^+\rangle_{CF} + |\Phi^+\rangle_{BF}|\Phi^+\rangle_{CE},\end{aligned} \tag{36}$$

and the normalization constant is $\mathcal{C} = \sqrt{d/(2(d+1))}$. Therefore, by projecting R onto $|\psi^*\rangle$, we see that any pure input state $|\psi\rangle$ transforms according to

$$\begin{aligned}|\psi\rangle \;\to\; &\mathcal{C}\left[\alpha|\psi\rangle_A(|\Phi^+\rangle_{BE}|\Phi^+\rangle_{CF} + |\Phi^+\rangle_{BF}|\Phi^+\rangle_{CE})\right.\\ &+\beta|\psi\rangle_B(|\Phi^+\rangle_{AE}|\Phi^+\rangle_{CF} + |\Phi^+\rangle_{AF}|\Phi^+\rangle_{CE})\\ &\left.+\gamma|\psi\rangle_C(|\Phi^+\rangle_{AE}|\Phi^+\rangle_{BF} + |\Phi^+\rangle_{AF}|\Phi^+\rangle_{BE})\right].\end{aligned}$$

It can be easily verified that this transformation is universal, i.e. the single-clone fidelities do not depend on the output state.

We can express the fidelities in terms of the coefficients α, β, and γ, by noting that

$$\begin{aligned}&\langle\lambda_{+,1}; kl|\Phi^+_{RA}\otimes\mathbb{1}_{BC}|\lambda_{+,1}; kl\rangle = (\alpha + \beta/d + \gamma/d)^2,\\ &\langle\lambda_{+,1}; kl|\Phi^+_{RB}\otimes\mathbb{1}_{AC}|\lambda_{+,1}; kl\rangle = (\beta + \alpha/d + \gamma/d)^2,\\ &\langle\lambda_{+,1}; kl|\Phi^+_{RC}\otimes\mathbb{1}_{AB}|\lambda_{+,1}; kl\rangle = (\gamma + \alpha/d + \beta/d)^2.\end{aligned} \tag{37}$$

Using the normalization condition (32), we obtain the fidelity triplet

$$\begin{aligned}F_A &= 1 - \frac{d-1}{d}\left[\beta^2 + \gamma^2 + \frac{2\beta\gamma}{d+1}\right],\\ F_B &= 1 - \frac{d-1}{d}\left[\alpha^2 + \gamma^2 + \frac{2\alpha\gamma}{d+1}\right],\\ F_C &= 1 - \frac{d-1}{d}\left[\alpha^2 + \beta^2 + \frac{2\alpha\beta}{d+1}\right].\end{aligned} \tag{38}$$

This, together with the normalization condition (32) and the constraints $\alpha \geq 0, \beta \geq 0, \gamma \geq 0$, provides a parametric description of the whole class of the optimal universal asymmetric $1 \to 3$ cloning machines in a Hilbert space of arbitrary dimension d.

As an example, in Fig. 1 we plot the trade-off between F_A and F_B for several different values of the fidelity of the third clone F_C for $1 \to 3$ asymmetric cloning of qubits, $d = 2$. Note, that in the limit where one of the three coefficients α, β, γ is equal to zero the asymmetric $1 \to 3$ cloning essentially reduces to the optimal asymmetric $1 \to 2$ cloning. However, even in this case the fidelity of the third clone is larger than $1/2$, which is what one could have naively expected. This interesting effect is clearly visible in Fig. 1. The endpoints of the curves showing the trade-off between F_A and F_B for a fixed F_C correspond to optimal $1 \to 2$ asymmetric cloning in the subspace of qubits A and C (or B and C). Note that the endpoints do not lie on the line $F_B = 1/2$ ($F_A = 1/2$) and the fidelity F_B (F_A) is thus higher than $1/2$ even in this limit case. This behavior can be easily understood by noting that in the $1 \to 2$ cloning, the ancilla (anti-clone) carries some information about the input and a third clone with fidelity larger than $1/2$ can be produced simply by applying the optimal approximate universal-NOT gate [26, 27] to the anti-clone. In particular, for $\alpha = \beta = 1/\sqrt{3}$ and $\gamma = 0$ we obtain the optimal triplet of fidelities $F_A = F_B = 5/6$ and $F_C = 5/9$. The three clones exhibiting these fidelities can be prepared by first performing the optimal symmetric $1 \to 2$ universal cloning which produces two clones with fidelity $5/6$. The third clone is then obtained from the anti-clone by applying the approximate UNOT which yields a clone with fidelity exactly $5/9$.

IV. CONCLUSIONS

In summary, we have investigated asymmetric universal cloning in arbitrary dimension. We have proved the optimality of the universal asymmetric $1 \to 2$ cloning machines that have been previously considered as possible efficient attacks on certain classes of quantum key distribution protocols. We have then extended the concept of asymmetric cloning to quantum triplicators, which produce three clones of different fidelity. We have derived a simple parametric description of the optimal asymmetric $1 \to 3$ cloning machines and we have provided an explicit formula for the optimal cloning transformation.

We anticipate that our results may play an important role in quantum information theory, for instance in the analysis of quantum information distribution in quantum networks and in studies of eavesdropping strategies on multi-party quantum communication protocols.

Acknowledgments

We acknowledge financial support from the EU under project SECOQC (IST-2002-506813) . JF and RF also acknowledge support from the grant MSM 6198959213 of the Czech Ministry of Education. NJC acknowledges financial support from the Communauté Française de Belgique under grant ARC 00/05-251 and from the IUAP programme of the Belgian government under grant V-18.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] W.K. Wootters and W.H. Zurek, Nature (London) **299**, 802 (1982); D. Dieks, Phys. Lett. **92A**, 271 (1982).
[3] V. Bužek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
[4] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).
[5] D. Bruss, A. Ekert, and C. Macchiavello, Phys. Rev. Lett. **81**, 2598 (1998).
[6] V. Bužek and M. Hillery, Phys. Rev. Lett. **81**, 5003 (1998).
[7] R.F. Werner, Phys. Rev. A **58**, 1827 (1998).
[8] V. Bužek, M. Hillery, and P. L. Knight, Fortschr. Phys. **48**, 521 (1998).
[9] N. J. Cerf, Acta Phys. Slov. **48**, 115 (1998); J. Mod. Opt. **47**, 187 (2000).
[10] C.S. Niu and R.B. Griffiths, Phys. Rev. A **58**, 4377 (1998).
[11] N.J. Cerf, Phys. Rev. Lett. **84**, 4497 (2000).
[12] S.L. Braunstein, V. Bužek, and M. Hillery, Phys. Rev. A **63**, 052313 (2001).
[13] R. Filip, Phys. Rev. A **69**, 032309 (2004); Phys. Rev. A **69**, 052301 (2004).
[14] C.-S. Niu and R.B. Griffiths, Phys. Rev. A **60**, 2764 (1999).
[15] C.A. Fuchs, N. Gisin, R.B. Griffiths, C.-S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).
[16] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A 59, 4238-4248 (1999).
[17] N.J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
[18] D. Bruss and C. Macchiavello, Phys. Rev. Lett. **88**, 127901 (2002).
[19] Z. Zhao, A.-N. Zhang, X.-Q. Zhou, Y.-A. Chen, C.-Y. Lu, A. Karlsson, and J.-W. Pan, quant-ph/0412017.
[20] S. Iblisdir, A. Acín, N. Gisin, J. Fiurášek, R. Filip, and N.J. Cerf, quant-ph/0411179.
[21] S. Iblisdir, A. Acín, and N. Gisin, quant-ph/0505152.
[22] J. Fiurášek, Phys. Rev. A **67**, 052314 (2003).
[23] L.-P. Lamoureux, P. Navez, J. Fiurášek, and N. J. Cerf, Phys. Rev. A **69**, 040301(R) (2004).
[24] J. Fiurášek, Phys. Rev. A **64**, 062310 (2001).
[25] J. Fiurášek, S. Iblisdir, S. Massar, and N. J. Cerf, Phys. Rev. A **65**, 040302 (2002).
[26] N. Gisin and S. Popescu, Phys. Rev. Lett. **83**, 432 (1999).
[27] V. Bužek, M. Hillery, and R.F. Werner, Phys Rev. A **60**, R2626 (1999).